Contract No. NASw - 572

Westinghouse Reference WGD - 38521

RESEARCH ON FAILURE FREE SYSTEMS

Quarterly Report No. 4

Covering the period July 20, 1964 to October 20, 1964

Prepared for:

The National Aeronautics and Space Administration
Washington, D. C.

Westinghouse Defense and Space Center

P. O. Box 1897 Baltimore 3, Maryland

Report Objective and Contract Status Statement

This quarterly report is prepared in accordance with the requirements of contract NASw-572, "Research on Failure-Free Systems", between the Westinghouse Electric Corporation and the National Aeronautics and Space Administration. The report describes the work which has been done on the four major tasks described by Amendment No. 1 of this contract. The period covered by this report corresponds to the second quarter of the contract extension established by the same Amendment. The work to date represents completion of approximately 40% of the anticipated effort.

A. PROGRAM OBJECTIVE

The general objective of this research program is to develop new techniques that will advance the state-of-the-art concerned with ultrareliable electronic systems. Techniques are being considered which are expected to result in significant increases in the reliability of vital electronic systems. These increases will be realized by giving the systems the capability to withstand a large percentage of internal component failures without degradation of system functional operation. The scope of this program includes the study of error detecting and error correcting codes, the problems associated with using redundant equipment, new schemes for permitting redundant system reorganization in response to changing failure patterns, adaptive logic networks and others.

B. ACTIVITY BY TASKS

The four major tasks of the current contract extension are:

I. Statistical measure of quality
II. Adaptive voter
III. Failure responsive system organizations
IV. Medium communication

A brief summary of the work proposed for each of these tasks is presented below with a review of the progress made to date on each task.

Task I. Statistical Measure of Quality

The object of this task is to develop a method for accurately evaluating the reliability of redundant systems which may contain internal component failures at the time the evaluation is made. Particular attention is to be given to making high confidence reliability estimates based on the analysis of partial system test results. Estimates based on partial system tests will soon be essential to the effective use of redundant systems because of the high cost of system failures and the high cost of delays required for complete tests.

The first goal of this task for the current year was the establishment of a suitable set of assumptions upon which the remaining effort on the task could be based. A set of assumptions has been established after careful consideration of a wide range of effects which might contribute to total estimation error. The resulting assumptions are intended to focus the study effort on the members of a class of systems which are most likely to be used in the field in the relatively near future. These assumptions are:

1. Only order-three redundant systems will be considered.
2. Systems are complex enough that exhaustive testing of each subsystem will not be feasible at the time of interest.

3. The individual subsystems fail at a constant rate; hence, they have exponential reliability functions.

4. The design failure rates will be assumed to be true.

5. The tests can be made rapidly enough so that no failures will occur during the test period.

In addition to establishing this set of assumptions, attention has also been given to defining the type of tests which is appropriate to systems of this class. This effort has been primarily oriented toward the elimination of test possibilities because of one or more basic incompatibilities between the test requirements and the basic operation of redundant systems.

In order to achieve the goals of the task, one or more statistical estimation techniques still have to be formulated based on the recognition of the error sources and the assumptions listed above. Also, test procedures must be developed which can provide input information appropriate to each of the estimation techniques.

Task II. Adaptive Voter

This task is concerned with the development of a new implementation of the restoring (or voting) circuits required by multiple-line redundant systems. It has been shown analytically that voting circuits with certain adaptive capabilities are potentially more effective in combating the effects of failures than are the currently used majority-voting circuits. The specific object of this task is to design, construct, and test an adaptive voting circuit which will include the most recent advances in adaptive circuit components which are known to the state-of-the-art.

As originally scheduled, the work on this task is not expected to begin until the the third quarter of the new contract period established by Amendment 1. Arrangements have been made, however, to procure thirty Mercury Cell Integrators from the Department of Defense for evaluation in adaptive voting circuits. These devices will be GFE at no cost to this contract.

Task III. Failure Responsive System Organizations

This task is intended to be a continuation of the "Self-Repairing Systems" study which began during the first year of this contract. It was shown in that study that systems which have the capability to partially reorganize their redundant subsystems in response to existing internal failure patterns may be more resistant to early life system failures than comparable fixed redundant systems. The first goal of this study is to develop design rules

and implementation techniques which will make such systems practicable. The second goal is to design a specific study vehicle which can be used to demonstrate the feasibility of such systems.

The computer simulation program which was briefly described in Quarterly Report No. 3 has been used to investigate a wide variety of feasible system reorganizational strategies. This investigation has resulted in the establishment of the following general design rules.

1. The mobility[1] of all of the individual subsystems should be as nearly equal as possible.
2. The subsystems which are available for use as spares (or replacements) to any two stages should be chosen so that the mutual dependence by the stages on the same spares is minimized.
3. The systems should be organized so that normally a subsystem will not move to the aid of a critically failed stage if its movement will leave the stage in which it is presently operating vulnerable to a single failure. A critically failed stage should have the "authority", however, to demand the movement of a spare subsystem if the movement of all of the spare subsystems available to this stage are restricted as above.

The simulation program has been used to confirm the hypothesis that many of the possible spare selection patterns are only superficially different. This means that the members of several sets of feasible selection patterns have exactly the same effect on system reliability.

The simulation study also has been extended to include orders of redundancy different from order-three. This includes fractional and even orders of redundancy. As an example of the results obtained from this portion of the study, it has been shown that three-and-one-half order[2] failure responsive systems are potentially much more reliable than order-five multiple-line majority-voted systems.

The use of reorganizational strategies which employ a "pool" of spare signal processors in an initially "off-line" operation has been avoided for a number of reasons. The most important reason is that no automatic checkout is provided for the spares in this pool, and, as a result, spares which are already failed can be called into use. This system could

---

1. "Mobility" is a measure, associated with individual subsystems, which indicates their relative capability to move to locations other than their original ones.
2. A "three-and-one-half" order system is a system initially having half its stages order-three and the other half order-four redundant.

allow two failed subsystems to control the majority vote of a stage, thus inadvertently failing the entire system.

Because the Mean Time Before Failure is not a particularly meaningful reliability measure for redundant systems with relatively short but vital missions, a new measure was adopted for comparing failure responsive systems. The measure is the time at which the reliability of the systems falls below some predetermined level. For this study, the .90 level has been used.

To normalize the time scale, all simulations have been restricted to systems whose non-redundant forms would be identical.

The curves shown in figure 1 demonstrate the effectiveness of the proper use of failure responsive reorganizational capability. The point labeled "A" on the ordinate represents the point at which the reliability of a multiple-line majority-voted system with perfectly reliable voters falls below the .90 level. Curve 1 is a smoothed out plot of .90 reliability time points for order three failure-responsive systems where the peripheral switching circuitry is assumed to be perfectly reliable. Curve 2 is an analogous plot for a similar system where the switching circuitry is assumed to compose approximately one half of total circuitry in the system. It can be seen from these curves that the reorganizational capability is quite effective, even under relatively pessimistic switching circuitry assumptions.

The details of the computer simulation program and the results of the simulations will be reported in a technical report to be issued within the next few weeks[3].

Task IV. Medium Communication for Module Reorganization

The primary goal of this task is to explore the advantages and limitations of systems which have the capability to relate their component subsystems through signals transmitted in a medium rather than over wired and switched signal paths. As part of the investigation, modules will be postulated which can select appropriate input signals from those found in the medium, and, in turn, supply output signals to the same medium. The object in performing this investigation is to determine if a technique such as this can be used to implement failure responsive systems in a more reliable manner than can be achieved using more standard techniques.

3. The report will also be submitted to the University of Pittsburgh by C. G. Masters (Principal Investigator) as a Masters Degree Thesis.

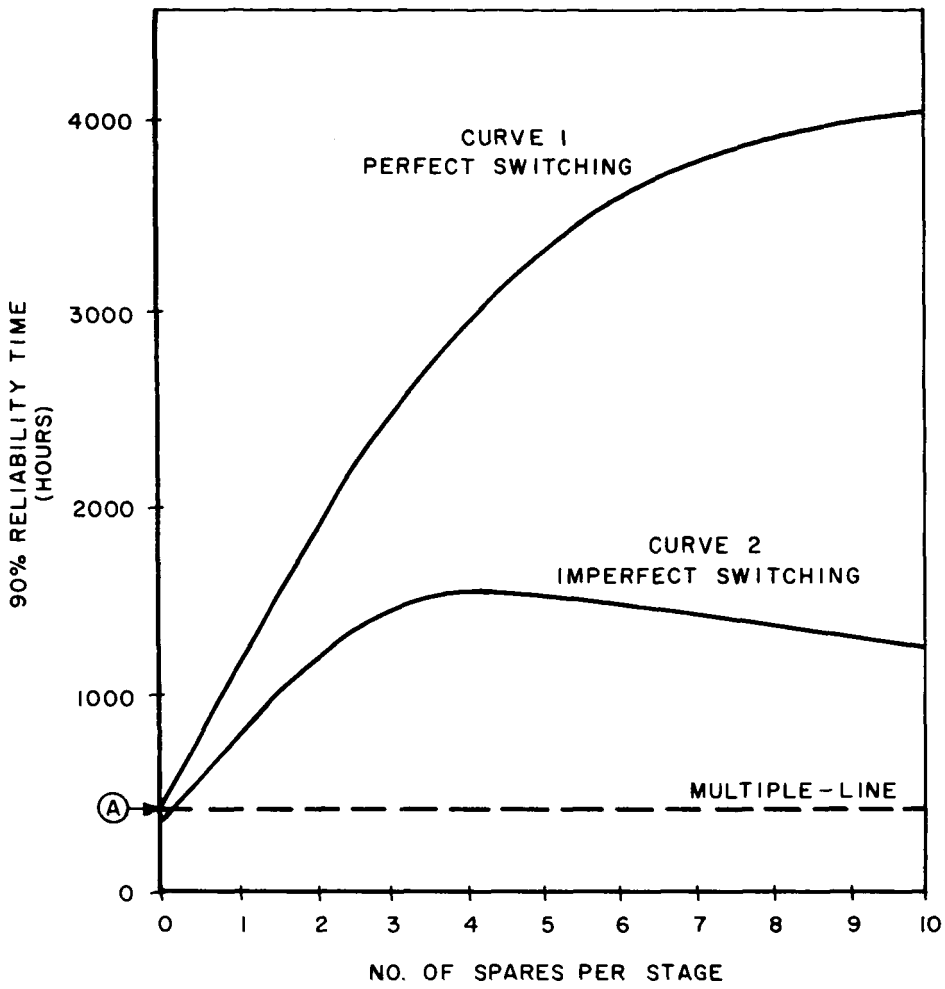


Figure 1. Comparison of Failure Responsive Systems (Solid Lines) and A Multiple Line System (Dashed Line)

The effort on this task was delayed because of a personnel scheduling problem. Active effort was begun on this Task on 16 October 1964. The only definite action taken so far on this task has resulted in the decision to orient the effort on this task toward the consideration of media containing memory.

D. MANAGEMENT AND PERSONNEL

The management of this contract continues to be performed by the Advanced Development Subdivision of the Surface Division of the Westinghouse Electric Corporation. The management personnel directly involved in the program include:

Mr. Sidney E. Lomax, Director of Development

Mr. Allen B. Walls, Supervisor

The technical personnel assigned to the program during this contract quarter include:

Mr. William C. Mann, Project Engineer

Mr. Harvey I. Eisenberg

Mr. Joseph M. Hannigan

Mr. Charles G. Masters, Jr.

Mr. Kevin P. Shambrook

CORRESPONDENCE ROUTING SLIP

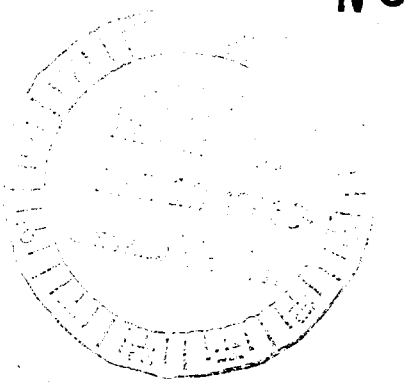
	Office Symbol	Name (if necessary)		Action
1		[illegible]		Approval
				Concurrence
				File
2		PROCESSING DEPT. (Input)		Information
				Investigate & Advise
3		DOCUMENT SERVICES (Req.Proc)		Note and Forward
				Note and Return
4				Per Request
				Recommendation
5				Coordination
				Signature
6				Reply for Signature of:
7				ARSOOK US: 990

Remarks: Attached Memo/Watson/4-4-66/Memorandum of Understanding for NASw-572

For appropriate action.

cc: M. Nagurney

N66-82715



From:

Staff Symbol	Name: I. Lebow	Date: 4-11-66

Facility Form 489 July, 1963